TECHNIQUE T804: BLOCK REPORTING MESSAGE

CyOTE Use Case(s)	MITRE ATT&CK for ICS® Tactic
Alarm Logs, HMI	Inhibit Response Function
Data Sources	
Potential Data Sources	Device/Application/System Logs, Network Protocol Analysis, Packet Capture, Zeek Logs, Alarm History, Data Historian
Historical Attacks	Industroyer/CRASHOVERRIDE[1]

TECHNIQUE DETECTION

The Block Reporting Message technique[2] (Figure 1) may be detected when expected reporting messages are not sent or when unauthenticated messages are being sent across these systems or devices.

To augment commercial sensor gaps, the CyOTE program has developed capabilities such as Proof of Concept tools[3] and Recipes[4] for asset owners and operators (AOO) to identify indicators of attack for techniques like Block Reporting Message within their operational technology (OT) networks. Referencing CyOTE Case Studies[5] of known attacks, AOOs in both small and large organizations can utilize CyOTE's Use Case analyses to tie operational anomalies and observables to cyber-attack campaigns resulting in ever-decreasing impacts.

PERCEPTION: OBSERVABLES FROM HISTORICAL ATTACKS

The Block Reporting Message technique was used in the Industroyer attack in the Ukraine in 2016.[6,7] In this attack, the following observables were identified:

- An increase of packet traffic
- Blocking of command messages
- Unnecessary messages sent to the data historian or to devices

Disclaimer: Past occurrences are not guaranteed to occur in future attacks.

---

[1] MITRE, Software: Industroyer, CRASHOVERRIDE, https://collaborate.mitre.org/attackics/index.php/Software/S0001
[2] MITRE ATT&CK for ICS, T804: Block Reporting Message, https://collaborate.mitre.org/attackics/index.php/Technique/T0804
[3] A Proof of Concept tool is a representative implementation of a set of steps and methods for identifying techniques. A Proof of Concept tool is defined as a script(code) or using capabilities of existing tools (e.g., Splunk, Gravwell), to demonstrate the capability to identify adversarial activity for a selected technique. A Proof of Concept tool is not ready for implementation in an AOO's environment as its major focus is to a specific instance (device, vendor, protocol, scenario) in order to prove a concept.
[4] A Recipe is a set of steps and methods for identifying techniques. Recipes can be used to develop a Proof of Concept or operational tool in an AOO's OT environment.
[5] Visit https://inl.gov/cyote/ for all CyOTE Case Studies.
[6] https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
[7] https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

COMPREHENSION

In the Industroyer attack, the adversary was able to block command and reporting messages once they had gained access to the Data Historian and initiated the compromise. They were able to issue unauthorized commands to cause impactful and damaging changes through the use of other techniques, including Device Restart/Shutdown, Service Stop, Manipulation of Control, and Manipulation of View.[8] By understanding the nature and possible origins of this attack, as well as how the adversary used the Block Reporting Message technique to execute the attack, an AOO can better comprehend how this technique is used with others and enhance their capabilities to detect attack campaigns using this technique and decrease an attack's impacts.

CURRENT CAPABILITY

The CyOTE Proof of Concept tool for Block Reporting Message performs deep packet inspection on Packet Captures (PCAPs) or live streams to identify and log packets indicative of blocked message reporting. These include the DNP3 command "Disable Spontaneous Messages" and the Modbus command "Force Listen Only Mode." Both commands are instructions to stop message reporting.

POTENTIAL ENHANCEMENTS

The CyOTE Proof of Concept tool could be expanded to cover more command types and function codes in DNP3, Modbus, and other frequently used industrial control system (ICS) protocols. The tool could also help distinguish traffic patterns in packets relevant to this technique.

ASSET OWNER DEPLOYMENT GUIDANCE

The operational tool should be able to be deployed on a host capable of processing the desired amount of traffic in an acceptable time frame. This host will either need access to a span port for live traffic or storage for PCAP files to be processed. The tool will need to be configured with information on the device to be monitored, such as the device vendor, model, and connection type.

AOOs can refer to the CyOTE Technique Detection Capabilities report (visit https://inl.gov/cyote/) for more information on the background and approach of CyOTE's technique detection capabilities.

AOOs can also refer to the CyOTE methodology for more information on CyOTE's approach to identifying anomalies in an OT environment, which, when perceived, initiates investigation and analysis to comprehend the anomaly.

Click for More Information	CyOTE Program || Fact Sheet || CyOTE.Program@hq.doe.gov
DOE Senior Technical Advisor	Edward Rhyne || Edward.Rhyne@hq.doe.gov || 202-586-3557

[8] CyOTE Case Study: CRASHOVERRIDE/Industroyer. Visit https://inl.gov/cyote/ for more information.

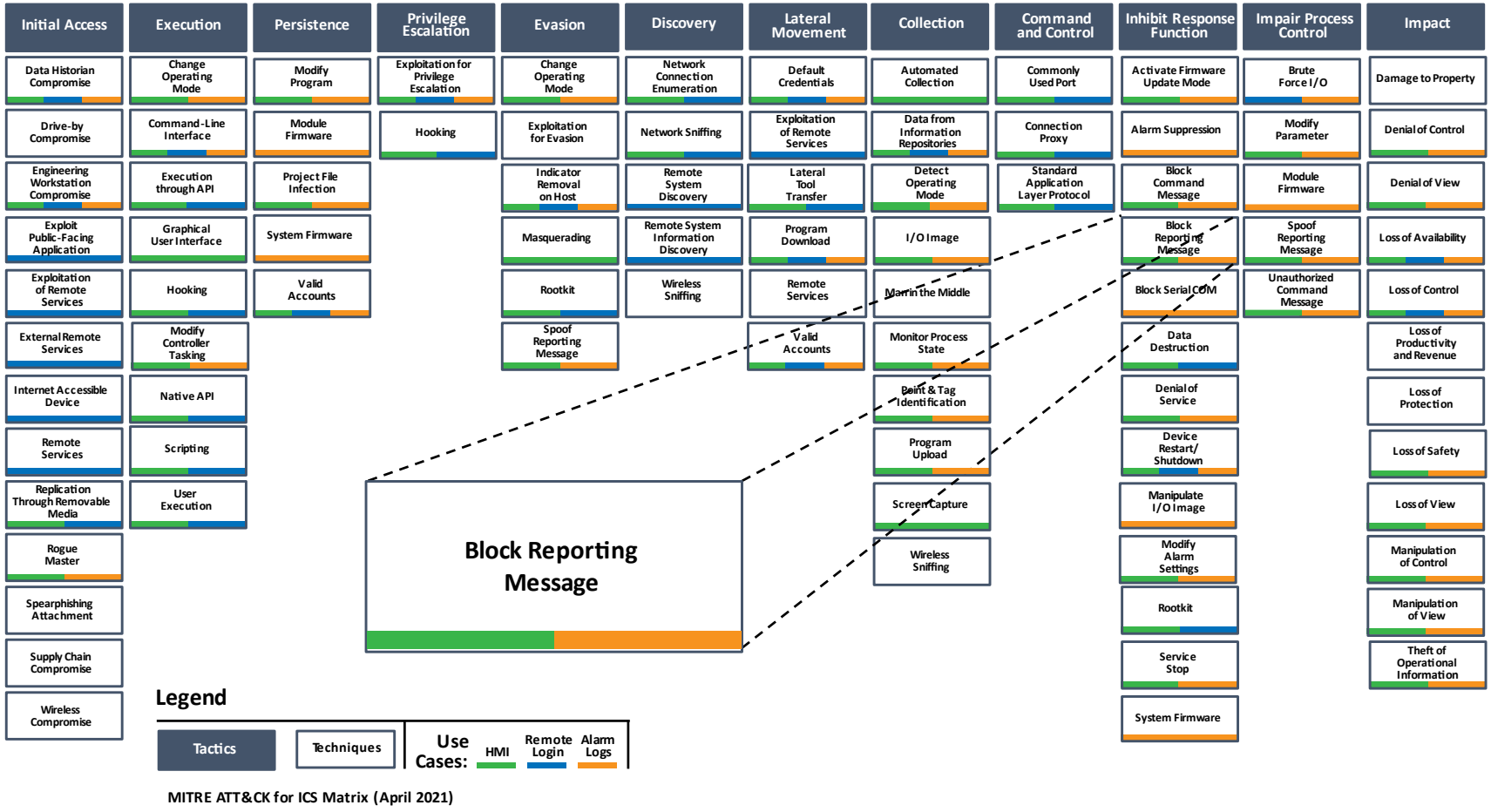

Figure 1: ICS ATT&CK Framework[9] – Block Reporting Message Technique

[9] © 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.